UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/562,036 | 07/10/2006 | Rached Ksontini | 90500-0000077/US | 6327 |

30593 7590 03/31/2009
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

| EXAMINER | |
|---|---|
| GELAGAY, SHEWAYE | |
| ART UNIT | PAPER NUMBER |
| 2437 | |
| MAIL DATE | DELIVERY MODE |
| 03/31/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/562,036 | **Applicant(s)**<br>KSONTINI ET AL. | |
| | **Examiner**<br>SHEWAYE GELAGAY | **Art Unit**<br>2437 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _22 December 2005_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _1-12_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-12_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _22 December 2005_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _12/22/05_.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to the applicant's preliminary amendment dated 12/22/2005. In the amendment claims 1-9 are amended, claims 10-12 are newly added.

2. Claims 1-12 are pending.

### Information Disclosure Statement PTO-1449

3. The Information Disclosure Statement submitted by applicant on 12-22-2005 has been considered. Please see attached PTO-1449.

### *Priority*

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

### Specification

4. The **disclosure** is objected to because of the following informalities:

It is not clear in the layout of the specification as where the back ground, summary or detailed description starts and ends.

Appropriate correction is required.

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), “Sequence Listings” (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A “MICROFICHE APPENDIX” (See MPEP § 608.05(a). “Microfiche Appendices” were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A “Sequence Listing” is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required “Sequence Listing” is not submitted as an electronic document on compact disc).

## *Claim Rejections - 35 USC § 103*

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naslund et al (hereinafter Naslund) US 2005/0278787 in view of Dierks US 6,948,061.

As per claim 1:

Naslund discloses a resource allocation method for a security module of an apparatus connected to a network, this network being administrated by an operator, said resources being used by application suppliers, the method comprising: receiving, by the operator, a request from a supplier and transmission of the request to the authority, this request comprising at least the supplier's public key; (page 4, pp. 55-57) transmitting, by the authority of at least the public key of the supplier to the operator; (page 4, pp. 55-57) transmitting, by the operator, a resource reservation instruction to the security module together with the supplier's public key; (page 4, pp. 55-57) transmitting, by the operator of the public key of the security module, to the supplier; (page 4, pp. 55) establishing a secure communication channel between the supplier and the security module; (page 4, pp. 55-57) loading of an application in the security module by the supplier; (page 4, pp. 57) and at least one of deactivating and clearing, by the operator, of at least part of the memory zone dedicated to a predefined resource when the clearing conditions are met. (page 6, pp. 78)

In addition, Naslund further discloses a digital rights management agent into a tamper-resistant identity module that is including standard SIM cards in GSM mobile telephones having a network operator and/or content provider authenticate the identity module including both symmetric and asymmetric encryption. An asymmetric pair may be used for encryption and authentication based on PKI. (pp. 79, 90) Naslund does not explicitly disclose generating a pair of asymmetric keys and storage of the private key in the security module, the public key being stored by an authority; and introducing at least one public key of the authority in the security module. Dierks in analogous art, however, disclose generating a pair of asymmetric keys and storage of the private key in the security module, the public key being stored by an authority; (col. 6, lines 20-26; token generate a key pair and have that key pair certified while the token is under the control of the end user … the private key is stored in a secure token) and introducing at least one public key of the authority in the security module; ( col. 6, lines 52-54; the corresponding public key is taken and certified by a CA) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Naslund with Dierks in order to generate a key pair at the secure module and have that key pair certified, thereby ensuring total control over the use of the private key from the moment of its generation. (col. 6, lines 20-24; Dierks)

As per claim 2:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Dierks further discloses wherein the pair of asymmetric keys is generated by the security module, the public key then being transmitted to the authority. (col. 6, lines 20-26; token generate a key pair and have that key pair certified while the token is under the control of the end user … the private key is stored in a secure token; col. 6, lines 52-54; the corresponding public key is taken and certified by a CA)

As per claim 3:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Naslund further discloses wherein the initialization parameters of a session key pertaining to the operator are stored in the security modules during the initialization. (page 4, pp. 55)

As per claim 4:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Naslund further discloses wherein the supplier transmits the initialization parameters of a session key to the operator, these parameters being transmitted to the security module during the reservation of a resource. (page 4, pp. 55)

As per claim 5:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Naslund further discloses wherein the establishment of a secure communication between the supplier and the security module is based on the use of the supplier's public key by the security module and the use of the security module's public key by the supplier. (page 4, pp. 57)

As per claim 6:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Naslund further discloses wherein the establishment of a secure communication between the operator and the security module is based on the generation of a session key using the initialization parameters of the operator. (page 4, pp. 55)

As per claim 7:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Naslund further discloses wherein the establishment of a secure communication between the supplier and the security module is based on the generation of a session key using the initialization parameters of the supplier. . (page 4, pp. 55)

As per claim 8:

The combination Naslund and Dierks teaches all the subject matter as discussed above. In addition, Naslund further discloses wherein the authority and the operator form the same entity. (page 4, pp.55; certified by a commonly trusted party)

3. Claims 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naslund et al (hereinafter Naslund) US 2005/0278787 in view of Dierks US 6,948,061 and in view of Sato et al. (hereinafter Sato) US 6,931,379.

As per claim 9:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the resource reservation instruction includes the sending of a domain key, which is specific to an application and common to all the security modules having this application, this key being used for the establishment of a secure communication between the supplier and the security module. Sato in analogous art, however, discloses wherein the resource reservation instruction includes the sending of a domain key, which is specific to an application and common to all the security modules having this application, this key being used for the establishment of a secure communication between the supplier and the security module. (col. 16, lines 6-15; the service provider encrypts the application by using the security domain public key and then transmits the encrypted application to IC card) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Naslund and Dierks with Sato in order to verify the validity of the application by the service provider. (col. 15, lines 60-66; Sato)

As per claim 10:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the deactivating or clearing of at least part of the memory zone dedicated to a predefined resource consist in clearing at least the public key of the supplier. Sato in analogous art, however, discloses wherein the deactivating or clearing of at least part of the memory zone dedicated to a predefined resource consist in clearing at least the public key of the supplier. (col. 8, lines 44-51; col. 9, lines 25-43; col. 13, lines 37-61) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Naslund and Dierks with Sato in order to provide a dynamic loading function capability of adding or deleting application after issuing of the IC card. (col. 1, lines 37-40; Sato)

As per claim 11:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the clearing conditions are met when the resource has been executed a number of time equal or greater than a predefined limit. Sato in analogous art, however, discloses wherein the clearing conditions are met when the resource has been executed a number of time equal or greater than a predefined limit. (col. 6, lines 3-8; when creating a security domain, the card issuer sets conditions of a cooperation contract in the security domain such as the number of times to load applications and a term of validity, and transmits the security domain to the partner of cooperation) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Naslund and Dierks with Sato in order to provide a dynamic loading function capability of adding or deleting application after issuing of the IC card while preventing an unauthorized user from loading an application. (col. 1, lines 37-40; col. 5, lines 21-22; Sato)

As per claim 12:

The combination Naslund and Dierks teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the clearing conditions are met when the resource has been executed a during a time equal or greater than a predefined time limit. Sato in analogous art, however, discloses wherein the clearing conditions are met when the resource has been executed a during a time equal or greater than a predefined time limit. (col. 6, lines 3-8; when creating a security domain, the card issuer sets conditions of a cooperation contract in the security domain such as the number of times to load applications and a term of validity, and transmits the security domain to the partner of cooperation) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Naslund and Dierks with Sato in order to provide a dynamic loading function capability of adding or deleting application after issuing of the IC card while preventing an unauthorized user from loading an application. (col. 1, lines 37-40; col. 5, lines 21-22; Sato)

## ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. G./
Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437